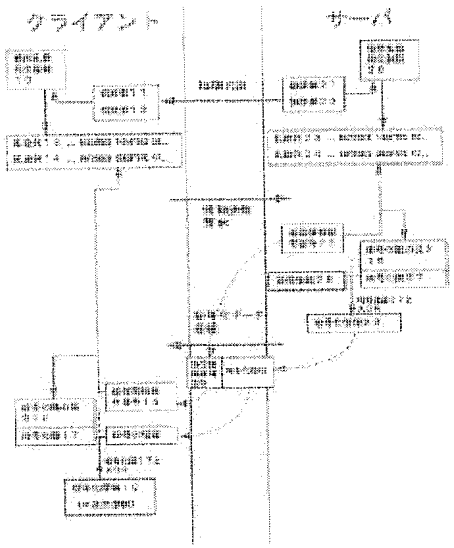
ENCRYPTION SYSTEM FOR DATA COMMUNICATION

Publication number: JP10145351 (A)
Publication date: 1998-05-29
Inventor(s): MANNAMI HIDESUKE; MIURA NAMIO
Applicant(s): HITACHI LTD
Classification:
- international: ***G06F13/00; H04L9/20;*** **G06F13/00; H04L9/18;** (IPC1-7): H04L9/20; G06F13/00
- European:
Application number: JP19960296156 19961108
Priority number(s): JP19960296156 19961108

Abstract of **JP 10145351 (A)**

PROBLEM TO BE SOLVED: To allow the system to apply high-speed processi ng to encryption and decoding with one instruction during c ommunication and to realize the encryption system with a high encryption security by allowing a transmitter side and a receiver side of a network system to possess a same initial value and a same pseudo-random number generating means, so as to produce a random number series. SOLUTION: A same pseudo-random number generating formula is possessed by both a transmitter side and a receiver side. At the start of communication, an initial value for encryption is transmitted, and a random number series is calculated. An encryption key 27 is decided, based on the random number string and a specific number of transmission information. Key information 27, and length 26 of the key are changed for each inform ation transmission.; Encryption is made for transmission information 28 by using the enc ryption key through exclusive OR (XOR) processing. The receiver side calculates a random number series similar to the case of the transmitter side to dec ide the key information. The transmitter side and th e receiver side possess the same initial value and the sam e pseudo-random number generating formula (to obtain the s ame key information) and use this k ey information to obtain decoding information 19.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－145351

(43)公開日　平成10年(1998)５月29日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　9/20		Ｈ０４Ｌ　9/00	６５３
Ｇ０６Ｆ　13/00	３５７	Ｇ０６Ｆ　13/00	３５７Ｚ

審査請求　未請求　請求項の数２　ＯＬ　（全５頁）

(21)出願番号　特願平8－296156

(22)出願日　平成８年(1996)11月８日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　万浪　秀祐
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内

(72)発明者　三浦　七三生
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内

(74)代理人　弁理士　小川　勝男

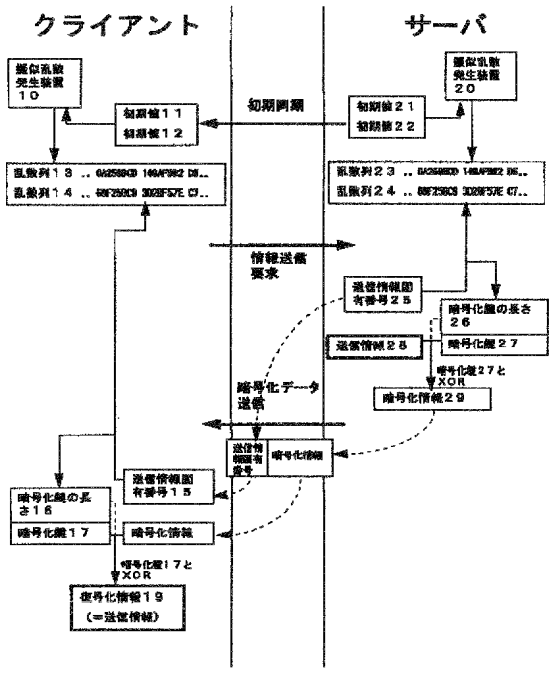
(54)【発明の名称】　データ通信の暗号化方式

(57)【要約】

【課題】ネットワークシステムの送信側と受信側において、同一の初期値と擬似乱数発生手段を所有して乱数列を発生させることにより通信中の暗号化および復号化処理を１命令にて高速処理し、かつ暗号強度の高い暗号化方式を実現する。

【解決手段】同一の擬似乱数発生公式を送信側、受信側の双方で所有しておく。通信の開始にあたって、暗号化の初期値を送信し、乱数列を計算する。この乱数列と送信情報の固有番号から暗号化鍵２７を決定する。鍵は毎回の情報送信ごとに鍵情報２７および鍵の長さ２６を変更する。送信情報２８はこの暗号化鍵を用いて排他的論理和（ＸＯＲ）により暗号化する。受信側ではね送信側と同様に乱数列を計算し、鍵情報を決定する。送信側と受信側は同じ擬似乱数発生公式と初期値を所有し（同じ鍵情報を得る）、この鍵情報を用いて復号化情報１９を得る。

図２



1

【特許請求の範囲】

【請求項１】通信回線を利用して情報を送受信するネットワークシステムの送信側と受信側において、同一の初期値と同一の擬似乱数発生手段を所有して乱数列を発生させることにより通信中の暗号化および復号化処理を１命令ないし数命令にて高速処理した暗号化方式。

【請求項２】インターネットのWWW（ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ）を利用して情報を送受信するシステムの送信側（サーバ）と受信側（クライアント）において、同一の初期値と同一の擬似乱数発生手段を所有して乱数列を発生させることにより通信中の暗号化および復号化処理を１命令ないし数命令にて高速処理した暗号化方式。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】送信側（サーバ）と受信側（クライアント）の間の通信情報を暗号化する情報処理システム。

【０００２】

【従来の技術】従来の技術では、暗号強度の強い暗号化方式（ＲＳＡ暗号やＤＥＳ暗号など）を採用すると、暗号化及び復号化のアルゴリズムは複雑となり、暗号化／復号化の処理時間に多くの処理時間を割かれていた。また、暗号化処理の処理時間の短いアルゴリズムを採用すると、暗号化の鍵の長さが一定のために暗号化情報を簡単に解読される恐れがあった。

【０００３】

【発明が解決しようとする課題】上記従来技術では、高トラヒックのデータ通信システムでは暗号強度の強い暗号化方式を採用することはできなかった。高トラヒックのデータ通信システムの暗号化方式は、暗号の強度を弱いものにするか、またはデータ通信のレスポンスタイムを犠牲にしながら暗号強度の強い方式を採用しなければならなかった。

【０００４】特にインターネットのWWW（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ）では、ＨＴＭＬで記述されたページに示された情報の送受信が可能であり、最近はメガバイト単位の情報を交換することも多くなってきているが、多くの情報は無暗号化状態で送受信されているか、または、強度の弱い暗号化によって送受信されている場合がほとんどである。

【０００５】本発明の目的は、暗号化処理をデータ通信のレスポンスタイムにほとんど影響を与えない程度に抑えつつ、かつ暗号強度の強い暗号化方式を実現することにある。

【０００６】

【課題を解決するための手段】図１は本発明の概念を示す図である。

【０００７】最初に同一の擬似乱数発生の公式を送信側、受信側の双方で所有しておく。通信の開始にあたって、まず暗号化の初期値を送信し、送信側及び受信側で乱数列を生成する。送信側では乱数列と送信情報の固有番号から乱数列を計算し、鍵情報を決定する。鍵情報は暗号強度を高めるために、毎回の情報送信ごとに鍵の内容および鍵の長さを変更する。

2

【０００８】送信情報本体は、この暗号化鍵を用いて簡単な命令群により暗号化する。ここでの簡単な命令群とは、排他的論理和（ＸＯＲ）などの１機械語命令または少数の機械語命令で構成される命令群のことである。

【０００９】受信側では、送信側と同様に暗号化の初期値と擬似乱数発生の公式から乱数列を生成し、受信情報の固有番号と乱数列から鍵情報を決定する。ここでは、通信の開始前に擬似乱数発生の公式と暗号化の初期値を共有しているため同じ乱数列を得ることができ、従って同じ鍵情報を得ることができる。これにより得た鍵情報を用いて、復号化の命令群（暗号化の命令群の逆変換）により復号化を行う。

【００１０】

【発明の実施の形態】本発明の実施の形態例を図表で説明する。

【００１１】図２は本発明の処理手順を示す図である。

【００１２】擬似乱数発生公式１０と擬似乱数発生公式２０は、同一のものをそれぞれクライアント側、サーバ側で記憶装置に保存しておく。

【００１３】擬似乱数発生の公式としては、M系列乱数列を利用し、特性多項式としては１回の排他的論理和で乱数が発生できる３項式を選んでおく。（例えば、ｆ（ｘ）＝１＋x^{32}＋x^{521}など。）また、乱数列の１つの値のビット数を３２ビットとしておく。

【００１４】データ通信の開始にあたって、サーバで初期値２１および初期値２２を決定し、これをクライアントに送信する。（初期同期）クライアントではこれらを初期値１１および初期値１２として保存する。初期値２１および初期値２２は３２ビットで表現できる任意の正の奇数にする。WWW（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ）での情報交換の場合、該当ＨＴＭＬページのロード時にこの初期同期を行う。クライアント側では、初期値１１および初期値１２を元にして、M系列乱数の特性多項式より、乱数列１３および乱数列１４を作成する。サーバ側でも同様に乱数列２３および乱数列２４を作成する。初期値が一致しているため、乱数列１３と乱数列２３、乱数列１４と乱数列２４は一致する。

【００１５】サーバはクライアントからの送信依頼を受け取ると、暗号化鍵情報の作成処理を開始する。乱数列２３と送信情報固有番号２５を利用して、暗号化鍵の長さ２６を作成する。この暗号化鍵の長さ２６は作成処理を短縮するために乱数列２３を元にした簡単な演算で作成する。例えば、乱数列２３の先頭から固有番号２５番目を利用する等。

【００１６】次に乱数列２４と送信情報固有番号２５を

利用して、暗号化鍵２７を作成する。この暗号化鍵２７は、暗号化鍵の長さ２６の値と同じ個数を作成する。

【００１７】この方法により決定した暗号化鍵の長さ２６と暗号化鍵２７とにより、送信情報２８の暗号化を行う。

【００１８】暗号化にあたっては、４バイト（＝３２ビット）ごとに排他的論理和（ＸＯＲ）のみを利用して暗号化し、暗号化に利用する機械命令を最短（１命令）にて行う。この処理を鍵を先頭から順番に利用しながら、暗号化鍵の長さ２６回行い、鍵を最後まで利用し終えると、また最初から鍵を再利用して暗号化して行く。これにより暗号化情報２９を得る。

【００１９】サーバは送信情報固有番号２５と暗号化情報２９をクライアントに送信する。

【００２０】復号化処理は、クライアントにて同様のことを行う。

【００２１】クライアントでは、まず乱数列１３と送信情報固有番号１５を利用して、暗号化鍵の長さ１６を作成し、乱数列１４と送信情報固有番号１５を利用して、暗号化鍵１７５を得る。

【００２２】この方法によりサーバで決定した暗号化鍵の長さ２６と暗号化鍵２７と同じものが得られる。

【００２３】復号化にあたっては、４バイトごとに、排他的論理和（ＸＯＲ）を利用して復号化し、復号化情報１９を得ることができる。この復号化情報１９の内容は送信情報２８の内容と一致する。

【００２４】

【発明の効果】本発明によれば、暗号化データ通信において以下の利点が得られる。

【００２５】（１）暗号化の通信ごとに鍵の長さを変えていてるので解読されにくい。

【００２６】従来の方法では高速な暗号化処理は、鍵の長さが一定のために通信文とその原文を１組入手されると鍵の解読が容易になされていた。本発明の方式では、通信文と原文を１組入手されても、その時に利用された初期値の特定は極めて困難である。

【００２７】（２）暗号化および復号化が高速

従来の暗号強度の強い暗号化方式では、変換単位（８バイト程度）ごとにビットシフトやビット反転を繰り返し、機械語命令で１０命令以上の処理を行うために暗号化および復号化の速度が遅かったが、本発明の方式では通信文の４バイト毎に機械語命令１命令で、暗号化及び復号化を行うため高速処理が可能である。

【図面の簡単な説明】

【図１】本発明の概念を示す図である。

【図２】本発明の処理手順を示す図である。

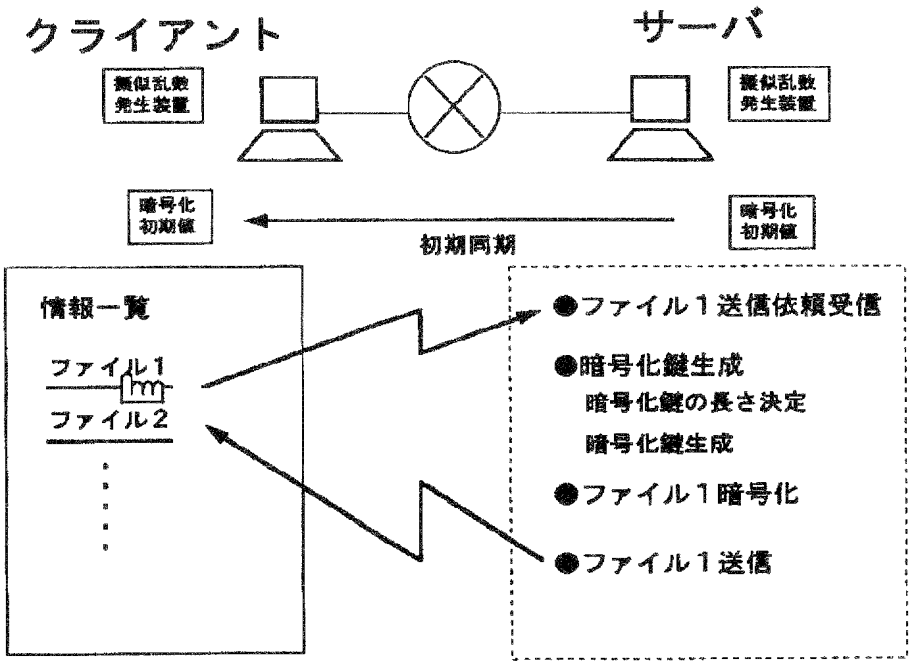
【符号の説明】

１０…擬似乱数発生公式（クライアント側）、１１…乱数列１３を発生させるための初期値、１２…乱数列１４を発生させるための初期値、１３…暗号化鍵の長さ１６を得るための乱数列、１４…暗号化鍵１７を得るための乱数列、１５…送信情報固有番号（クライアント側）、１６…暗号化鍵の長さ（クライアント側）、１７…暗号化鍵（クライアント側）、　　１９…復号化情報、２０…擬似乱数発生公式（サーバ側）、２１…乱数列２３を発生させるための初期値、２２…乱数列２４を発生させるための初期値、２３…暗号化鍵の長さ２６を得るための乱数列、２４…暗号化鍵２７を得るための乱数列、２５…送信情報固有番号（サーバ側）、２６…暗号化鍵の長さ（サーバ側）、　　２７…暗号化鍵（サーバ側）、２８…送信情報、

２９…暗号化情報。

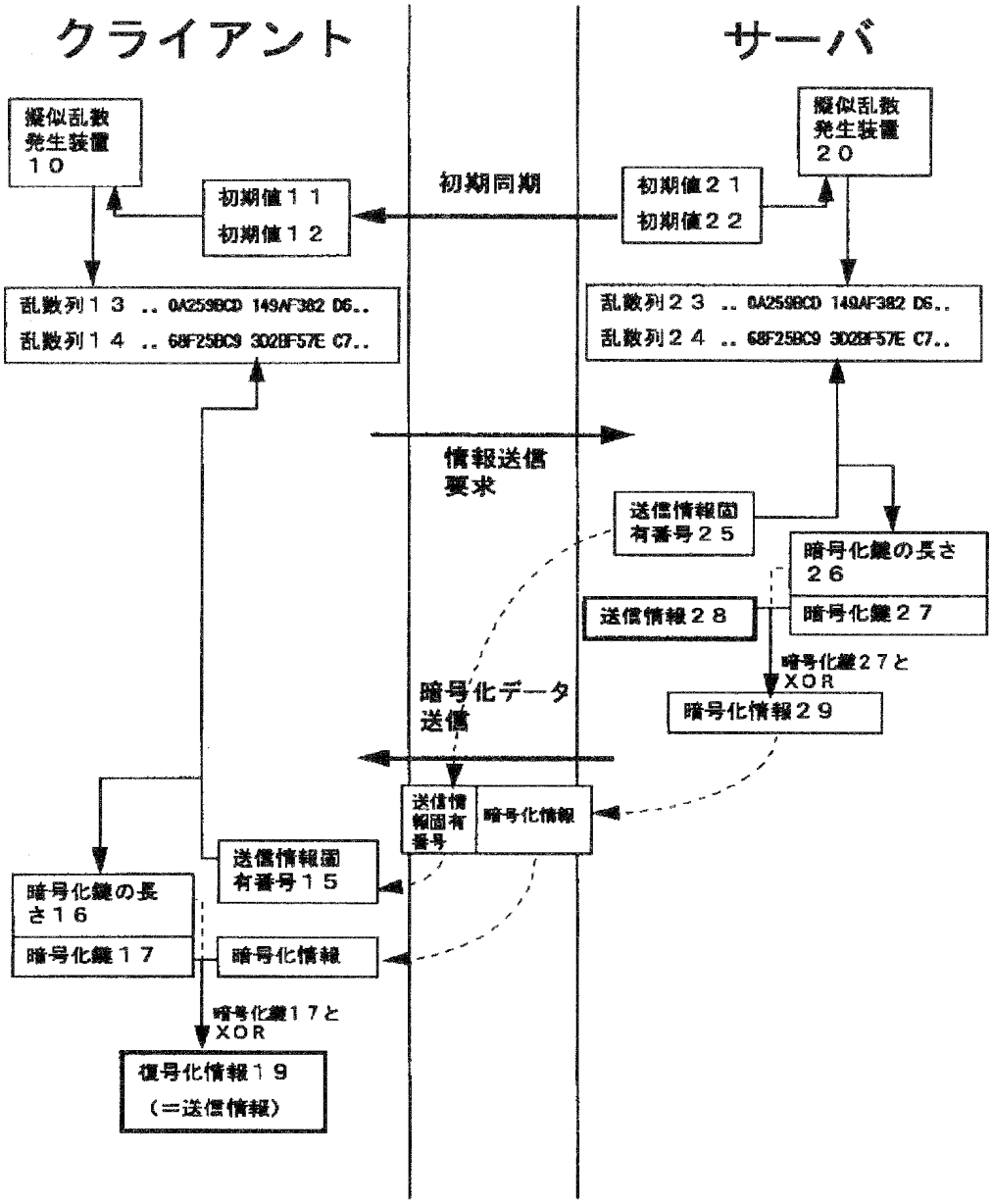
【図１】

図１


クライアント
サーバ
擬似乱数発生装置
擬似乱数発生装置
暗号化初期値
暗号化初期値
初期同期
情報一覧
ファイル1
ファイル2
●ファイル１送信依頼受信
●暗号化鍵生成
暗号化鍵の長さ決定
暗号化鍵生成
●ファイル１暗号化
●ファイル１送信

【図２】

図２


クライアント
サーバ
擬似乱数発生装置１０
擬似乱数発生装置２０
初期同期
初期値１１
初期値１２
初期値２１
初期値２２
乱数列１３ .. 0A259BCD 149AF382 D6..
乱数列１４ .. 68F25BC9 3D2BF57E C7..
乱数列２３ .. 0A259BCD 149AF382 D6..
乱数列２４ .. 68F25BC9 3D2BF57E C7..
情報送信要求
送信情報固有番号２５
暗号化鍵の長さ２６
暗号化鍵２７
送信情報２８
暗号化鍵２７とXOR
暗号化情報２９
暗号化データ送信
送信情報固有番号
暗号化情報
送信情報固有番号１５
暗号化鍵の長さ１６
暗号化鍵１７
暗号化情報
暗号化鍵１７とXOR
復号化情報１９
（＝送信情報）